

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-313056

(43)Date of publication of application : 09.11.1999

(51)Int.Cl.

H04L 9/08

G07B 15/00

G09C 1/00

G09C 1/00

H04L 9/32

(21)Application number : 11-047162

(71)Applicant : MATSUSHITA ELECTRIC IND CO
LTD

(22)Date of filing : 24.02.1999

(72)Inventor : TATEBAYASHI MAKOTO

(30)Priority

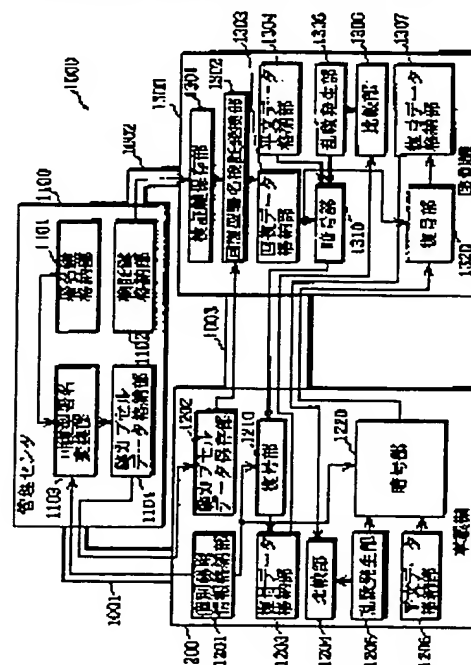
Priority number : 10 43230 Priority date : 25.02.1998 Priority country : JP

(54) EQUIPMENT CERTIFICATION AND CRYPTOGRAPHIC COMMUNICATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a system keeping high safety even if there is unjust invasion to system side equipment or analysis for equipment authentication or cryptographic communication between user side equipment and system side equipment.

SOLUTION: A control center 1100 prepares key capsule data and distributes them to the user side equipment by performing recovery type signature translation concerning personal secret information stored in the user side equipment (on-board equipment 1200) and distributes a prescribed key to the system side equipment (road side equipment 1300). The user side equipment transmits the key capsule data to the system side equipment and while using the verify key, the system side equipment restores the personal secret information from the key capsule data through signature verify translation. Since the user side equipment and system side equipment transmit data while enciphering them or decipher data while receiving them based on a secret key encipher algorithm while using the shared personal secret information as a key, the equipment certification and cryptographic communication can be performed between both the equipment.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of
rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-313056

(43) 公開日 平成11年(1999)11月9日

(51) Int.Cl. ⁸	識別記号	F I	
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 A
G 0 7 B 15/00	5 1 0	G 0 7 B 15/00	5 1 0
G 0 9 C 1/00	6 2 0	G 0 9 C 1/00	6 2 0 A
	6 4 0		6 4 0 B
H 0 4 L 9/32		H 0 4 L 9/00	6 0 1 E

審査請求 未請求 請求項の数10 O L (全 14 頁) 最終頁に続く

(21) 出願番号 特願平11-47162

(22) 出願日 平成11年(1999) 2 月24日

(31) 優先権主張番号 特願平10-43230

(32) 優先日 平10(1998) 2 月25日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 館林 誠

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

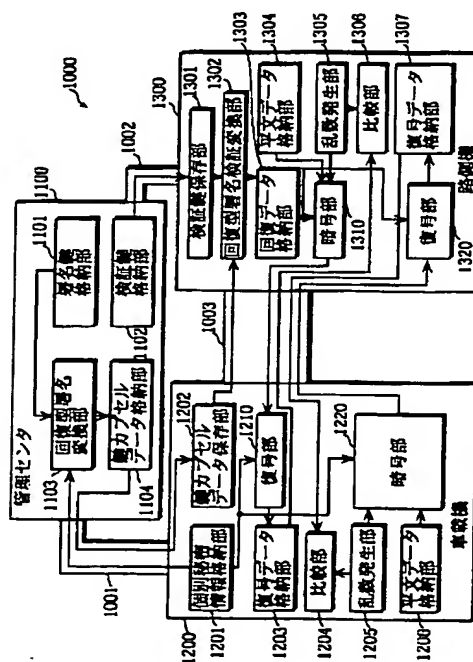
(74) 代理人 弁理士 中島 司朗 (外 1 名)

(54) 【発明の名称】 機器認証及び暗号通信システム

(57) 【要約】

【課題】 ユーザ側機器とシステム側機器の間での機器認証及び暗号通信に関して、システム側機器への不正な侵入や解析に対しても高度の安全性を保つシステムを提供する。

【解決手段】 管理センタ1100は、ユーザ側機器（車載機1200）が記憶する個別秘密情報に対して回復型署名変換を行って鍵カプセルデータを作成してユーザ側機器に配布し、所定鍵をシステム側機器（路側機1300）に配布する。ユーザ側機器は、前記鍵カプセルデータをシステム側機器に送信し、システム側機器は、前記検証鍵を用いて署名検証変換により前記鍵カプセルデータから前記個別秘密情報を復元する。ユーザ側機器とシステム側機器とが、共有した個別秘密情報を鍵として用い秘密鍵暗号アルゴリズムに基づき、データを暗号化して送信、又はデータを受信して復号することにより両者間で機器認証及び暗号通信を行う。



【特許請求の範囲】

【請求項 1】 機器認証及び暗号通信を行う機器認証及び暗号通信システムであって、

各ユーザ側機器毎に異なる個別秘密情報それぞれに対して、所定の変換を行うことにより鍵カプセルデータを作成して、各鍵カプセルデータを該当ユーザ側機器に配布し、前記各鍵カプセルデータから前記各個別秘密情報を復元するために用いる 1 つの所定鍵をシステム側機器に配布する管理装置と、

各ユーザ側機器は、前記個別秘密情報を記憶しており、機器認証及び暗号通信を行う際に、前記管理装置により配布された前記鍵カプセルデータをシステム側機器に送信する複数のユーザ側機器と、

前記ユーザ側機器から前記鍵カプセルデータを受信すると、前記管理装置により配布された前記所定鍵を用いて当該鍵カプセルデータから前記個別秘密情報を復元するシステム側機器とを備え、

前記ユーザ側機器は前記記憶している個別秘密情報を鍵として用い、前記システム側機器は前記復元した個別秘密情報を鍵として用いて、秘密鍵暗号アルゴリズムに基づく暗号化又は復号を行うことにより、前記機器認証及び暗号通信を行うことを特徴とする機器認証及び暗号通信システム。

【請求項 2】 前記管理装置は、回復型署名変換方法における署名鍵とこれに対応する検証鍵とを予め記憶しており、

前記所定の変換は、前記署名鍵を用いてなされる回復型署名変換であり、

前記所定鍵は、前記検証鍵であり、

前記システム側機器は、前記所定鍵を用いて前記回復型署名変換に対応する回復型署名検証変換を行うことにより当該鍵カプセルデータから前記個別秘密情報を復元することを特徴とする請求項 1 記載の機器認証及び暗号通信システム。

【請求項 3】 前記機器認証は、前記ユーザ側機器及び前記システム側機器のうち的一方である第 1 機器が乱数データを前記秘密鍵暗号アルゴリズムに基づき暗号化して、他方の第 2 機器に送信し、これを受信した第 2 機器が暗号化された乱数データを前記秘密鍵暗号アルゴリズムに基づき復号して応答データを作成し第 1 機器に返信し、前記応答データを受信した第 1 機器が当該応答データと前記乱数データとを比較することにより行われることを特徴とする請求項 2 記載の機器認証及び暗号通信システム。

【請求項 4】 前記回復型署名変換及び前記回復型署名検証変換は、楕円曲線理論に基づくものであることを特徴とする請求項 3 記載の機器認証及び暗号通信システム。

【請求項 5】 前記ユーザ側機器は、車に備えられる車載機であり、

前記システム側機器は、道路に設けられた路側機であり、

前記ユーザ側機器と前記システム側機器との間でのデータ送受信は、前記ユーザ側機器が前記システム側機器の付近を通過する際に行われることを特徴とする請求項 4 記載の機器認証及び暗号通信システム。

【請求項 6】 前記ユーザ側機器と前記システム側機器との間での機器認証は、相互に相手側機器を認証するものであり、

前記ユーザ側機器と前記システム側機器との間での暗号通信は、双方向に行われることを特徴とする請求項 5 記載の機器認証及び暗号通信システム。

【請求項 7】 前記管理装置は、複数の前記個別秘密情報を該当ユーザ側機器に配布し、

前記ユーザ側機器が記憶している前記個別秘密情報は、前記管理装置から配布されたものであることを特徴とする請求項 4 記載の機器認証及び暗号通信システム。

【請求項 8】 前記管理装置は、公開鍵暗号方法における公開鍵とこれに対応する秘密鍵とを予め記憶しており、

前記所定の変換は、前記公開鍵を用いてなされる公開鍵暗号変換であり、

前記所定鍵は、前記秘密鍵であり、

前記システム側機器は、前記所定鍵を用いて前記公開鍵暗号変換に対応する復号変換を行うことにより当該鍵カプセルデータから前記個別秘密情報を復元することを特徴とする請求項 1 記載の機器認証及び暗号通信システム。

【請求項 9】 前記ユーザ側機器は、車に備えられる車載機であり、

前記システム側機器は、道路に設けられた路側機であり、

前記ユーザ側機器と前記システム側機器との間でのデータ送受信は、前記ユーザ側機器が前記システム側機器の付近を通過する際に行われることを特徴とする請求項 8 記載の機器認証及び暗号通信システム。

【請求項 10】 機器認証及び暗号通信用の鍵である個別秘密情報を記憶する複数のユーザ側機器のいずれかから、システム側機器に対して前記個別秘密情報を配送する鍵配送方法であって、

各ユーザ側機器についての前記個別秘密情報に対して回復型署名変換を行うことにより鍵カプセルデータを作成して、該当ユーザ側機器に配布する鍵カプセルデータ作成及び配布ステップと、

前記回復型署名変換に対応する署名検証変換に用いる検証鍵を前記システム側機器に配布する検証鍵配布ステップと、

前記ユーザ側機器によりなされ、前記鍵カプセルデータ作成及び配布ステップにより配布された前記鍵カプセルデータを前記システム側機器に送信する鍵カプセルデー

タ送信ステップと、

前記鍵カプセルデータ送信ステップにより送信された鍵カプセルデータを受信し、前記検証鍵配布ステップにより配布された前記検証鍵を用いて当該鍵カプセルデータから前記個別秘密情報を復元する鍵復元ステップとを含むことを特徴とする鍵配送方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、複数のユーザ側機器のいずれかとシステム側機器の間で、互いに相手側機器の正当性を確認し、秘密にデータを送受信する機器認証及び暗号通信システムに関する。

【0002】

【従来の技術】一般に、価値のあるデータの通信においては、セキュリティの確保が重要な課題となる。即ち、価値のあるデータを通信相手に伝送する場合には、通信相手の機器が正当なものであることを確認することが必要であり、また、そのデータは、通信路上で第三者により不正に盗用又は改ざんされることから守られなければならない。

【0003】このようなセキュリティの確保が重視されるデータ通信システムの典型例として、無線通信を用いた高速道路の料金自動収受システムを挙げることができる。

<高速道路料金自動収受システム>以下、通常考えられる高速道路料金自動収受システムについて説明する。この高速道路料金自動収受システムは、高速道路の利用料金の支払いを、車に備えられる車載機と、高速道路の各入口又は出口の料金所ゲートに備えられる路側機との間の無線通信により行うものである。

【0004】車載機には着脱可能なICカードが備えられる。このICカードはプリペイドカードの機能を持ち当初所定の金額を示す残額情報が記録されている。高速道路の入り口のゲート（以下「入路ゲート」という。）においては、車載機は路側機に対して車載機IDを無線で送信し、路側機は車載機に対しては、ゲートID、入路時刻等を含む入路情報を無線で送信する。車載機は路側機から入路情報を受信すると、この入路情報をICカードに記録する。

【0005】一方、出口のゲート（以下「出路ゲート」という。）においては、車載機は路側機に対して入路情報と残額情報を無線で送信し、路側機は受信した入路情報に基づいて高速道路の利用料金を計算して、受信した前記残額情報からその利用料金を差し引いて残額情報を更新して、更新後の残額情報を車載機に対して無線で送信する。

【0006】なお、高速道路料金自動収受システム中に存在する車載機の数数は数百万台、路側機の数数は数千台であることが想定される。また、車載機と路側機との間の無線通信が可能な範囲は数十メートル程度であり、入路

ゲート及び出路ゲートにおいて車載機を搭載した車は料金支払い等のために停止する必要はない。従って、入出路ゲート付近における交通の混雑は軽減される。

【0007】このような高速道路料金自動収受システムが首尾良く運用されるためには、誤まりのない高速な無線通信が実現されることは当然であるが、それ以外にも次のようなセキュリティ面での課題が解決されることが必要となる。まず、路側機は、車載機が正当なものであることを認証しなければならない。偽の車載機による通信に対してはこれが偽物であることを直ちに判定し、ゲートを封鎖する、或いは車両番号を記録すると共に運転者の写真を撮る等の対抗措置がとられなければならない。

【0008】これと逆に、車載機は、路側機が正当なものであることを認証する必要もある。偽の路側機が車載機との通信を行うことにより、ICカード内に記録されている入路情報を書き換え、本来あるべき区間よりも短い区間の料金を支払う等の不正に利益を得るような試みを防止する必要があるからである。また、車載機と路側機との無線通信の内容が第三者に傍受され、その内容が不正に利用されることがあってはならない。

【0009】<秘密情報等の共有による通信セキュリティ確保>上述したセキュリティ面での課題は、一般に知られている機器認証及び暗号通信の技術を用いて、車載機と路側機との間でのデータの無線伝送を行うことで解決できる。例えば、車載機と路側機の間で、ある秘密鍵暗号アルゴリズムとある秘密情報とが共有されていればよい。通常この秘密情報は、暗号鍵又は復号鍵と呼ばれる。車載機と路側機の間で秘密鍵暗号アルゴリズムと秘密情報とが共有されていれば、これを用いて、相互に機器認証を行うことや、データ送信の際にはデータを暗号化して送信し、データ受信の際には受信したデータを復号すること等が可能となるからである。

【0010】なお、このような秘密鍵暗号アルゴリズムに基づく暗号化及び復号は、公開鍵暗号アルゴリズムと比べて小さな計算能力しか必要とせず、結果的に高速な処理が可能となるため、車の停止を要しないで自動的に料金収受を行う高速道路料金自動収受システムにおいて秘密鍵暗号アルゴリズムに基づく暗号通信を行うことは有効である。

【0011】但し、上述した高速道路料金自動収受システムにおいてはシステム中に車載機が複数存在するので、各車載機には車載機毎に異なる秘密情報をもたせる必要がある。なぜなら、もし、ある車載機Aの秘密情報と車載機Bの秘密情報とが同じであるとすれば、万一、車載機Aの内容が悪意ある第三者により解析され偽物の車載機A'ができた場合に、この偽物A'の不正利用を排除するためにネガティブリストを用いて車載機A'の不正利用を防止しようとすると、同時に正当な車載機Bの利用まで排除されてしまうからである。

【0012】

【発明が解決しようとする課題】ここで、各車載機毎に異なる秘密情報を、車載機と共有するために路側機がどのようにしてその秘密情報を獲得するかが問題となる。例えば、路側機に全ての車載機のIDと秘密情報とを対応づけた情報を予め記憶させておく方法が考えられる。しかし、この方法には、システム中に存在する数千台の路側機の記憶内容を更新する場合の負担が非常に大きい上に、万一、1つの路側機が悪意ある第三者により解析された場合に、全ての車載機の秘密情報がすべて暴露されてしまうという欠点がある。

【0013】また、別の方法として、車載機の秘密情報は車載機のIDからある秘密関数 f により導き出されるものであり車載機にはその関数値 $f(ID)$ が記録され、路側機にその秘密関数 f が備えられ、路側機は車載機のIDの通知を受けてこれから車載機の秘密情報を導き出すという方法が考えられる。しかし、この方法にも、万一、1つの路側機が悪意ある第三者により解析された場合に、秘密関数 f が暴露され、この結果として全ての車載機の秘密情報が暴露されてしまうという欠点がある。

【0014】なお、このような問題は、高速道路料金自動収受システム以外であっても、複数のユーザ側装置のいずれかと複数のシステム側装置のいずれかとの間でセキュリティを確保した通信を行うために、そのユーザ側機器とそのシステム側機器の間で秘密情報を共有する必要のあるシステムにおいては、同様に問題となる。そこで、本発明は、上述の問題点に鑑みてなされたものであり、ユーザ側機器とシステム側機器の間での機器認証及び暗号通信に関して、システム側機器への不正な侵入及び解析に対しても高度の安全性を保ち得る通信セキュリティ機能を有する機器認証及び暗号通信システムを提供することを第1の目的とする。また、このような機器認証及び暗号通信を秘密鍵暗号アルゴリズムに基づく暗号化又は復号を利用する場合において、その暗号化又は復号のための鍵を、システム側機器への不正な侵入及び解析に対する安全性が保てるように配送する鍵配送方法を提供することを第2の目的とする。

【0015】

【課題を解決するための手段】上記第1の目的を達成するために本発明に係る機器認証及び暗号通信システムは、機器認証及び暗号通信を行う機器認証及び暗号通信システムであって、各ユーザ側機器毎に異なる個別秘密情報それぞれに対して、所定の変換を行うことにより鍵カプセルデータを作成して、各鍵カプセルデータを該当ユーザ側機器に配布し、前記各鍵カプセルデータから前記各個別秘密情報を復元するために用いる1つの所定鍵をシステム側機器に配布する管理装置と、各ユーザ側機器は、前記個別秘密情報を記憶しており、機器認証及び暗号通信を行うに際して、前記管理装置により配布され

た前記鍵カプセルデータをシステム側機器に送信する複数のユーザ側機器と、前記ユーザ側機器から前記鍵カプセルデータを受信すると、前記管理装置により配布された前記所定鍵を用いて当該鍵カプセルデータから前記個別秘密情報を復元するシステム側機器とを備え、前記ユーザ側機器は前記記憶している個別秘密情報を鍵として用い、前記システム側機器は前記復元した個別秘密情報を鍵として用いて、秘密鍵暗号アルゴリズムに基づく暗号化又は復号を行うことにより、前記機器認証及び暗号通信を行うことを特徴とする。

【0016】上記構成により、システム側機器は、ユーザ側機器から送られる鍵カプセルデータからユーザ側機器毎に異なるものである個別秘密情報を復元するので、全てのユーザ側機器について、個別秘密情報とユーザ側機器のID等と対応づけて記憶していなくても、ユーザ側機器との間で機器の正当性の認証と暗号通信とを行うことができる。従って、システム側機器には全てのユーザ側機器についての個別秘密情報を記憶しないようにすることができるため、この場合、悪意ある者がシステム側機器に不正に侵入し解析を行ったとしても、その者は全てのユーザ側機器についての個別秘密情報を入手することはできない。

【0017】また、上記第2の目的を達成するために本発明に係る鍵配送方法は、機器認証及び暗号通信の鍵である個別秘密情報を記憶する複数のユーザ側機器のいずれかから、システム側機器に対して前記個別秘密情報を配送する鍵配送方法であって、各ユーザ側機器についての前記個別秘密情報に対して回復型署名変換を行うことにより鍵カプセルデータを作成して、該当ユーザ側機器に配布する鍵カプセルデータ作成及び配布ステップと、前記回復型署名変換に対応する署名検証変換に用いる検証鍵を前記システム側機器に配布する検証鍵配布ステップと、前記ユーザ側機器によりなされ、前記鍵カプセルデータ作成及び配布ステップにより配布された前記鍵カプセルデータを前記システム側機器に送信する鍵カプセルデータ送信ステップと、前記鍵カプセルデータ送信ステップにより送信された鍵カプセルデータを受信し、前記検証鍵配布ステップにより配布された前記検証鍵を用いて当該鍵カプセルデータから前記個別秘密情報を復元する鍵復元ステップとを含むことを特徴とする。

【0018】上記処理構成により、システム側機器が全てのユーザ側機器について、個別秘密情報とユーザ側機器のID等と対応づけて記憶していなくても、ユーザ側機器との間で機器の正当性の認証と暗号通信とを行うことができ、また、システム側機器への不正な侵入及び解析により不正に回復型署名についての署名検証変換用の検証鍵を得ることはできたととしても、その検証鍵からは回復型署名変換に用いる署名鍵が導き出せないで、悪意ある者による鍵カプセルデータの偽造が不可能となる。

【0019】

【発明の実施の形態】以下、本発明の実施の形態について、図を用いて説明する。

<構成>図1は、本発明の実施の形態に係る高速道路料金自動收受システム1000の主要部分の機能構成図である。

【0020】高速道路料金自動收受システム1000は、高速道路の利用料金の支払いを、車に備えられる車載機と、高速道路の各入口又は出口の料金所ゲートに備えられる路側機との間の無線通信により行うシステムであり、1つの管理センタ1100と数百万台の車載機と数千台の路側機とを備える。車載機と路側機との間の距離が数十メートル以内である限り車載機を搭載した車が移動中であっても無線通信が可能である。なお、同図は、1台の車載機1200と、1台の路側機1300と、管理センタ1100の関係に着目して示したものである。

【0021】<管理センタ>管理センタ1100は、システム内の全機器の正当性についての管理をするセンタであり、CPU、メモリ等を備えたコンピュータで構成され、車載機1200及び路側機1300との間で、秘密通信路1001及び1002を介して秘密にデータ通信を行うことができる。ここで、秘密通信路1001及び1002は、これを通るデータが悪意ある第三者に盗聴されたり改ざんされたりすることがないような高度のセキュリティ機能を有する通信路である。

【0022】管理センタ1100は機能的には、署名鍵格納部1101と、検証鍵格納部1102と、回復型署名変換部1103と、鍵カプセルデータ格納部1104とを備え、各機能は前記メモリにより、又は前記メモリに格納された制御用プログラムが前記CPUに実行されることにより実現されるものである。ここで、署名鍵格納部1101は、回復型署名アルゴリズムによりデジタル署名を行う際に用いる署名鍵Scを格納しているメモリ領域であり、検証鍵格納部1102は、前記署名鍵に対応し、デジタル署名を検証するための検証鍵Vcを格納しているメモリ領域である。

【0023】回復型署名変換部1103は、秘密通信路1001を介して車載機1200により送信された車載機個別秘密情報Kiを受け取り、この車載機個別秘密情報Kiに対して署名鍵Scを用いて回復型署名変換を行うことにより鍵カプセルデータCiを作成するものである。なお、回復型署名変換については後述する。また、鍵カプセルデータ格納部1104は、回復型署名変換部1103により作成された鍵カプセルデータCiを格納するメモリ領域である。

【0024】この他に管理センタ1100は、車載機からの車載機個別秘密情報Kiの受信、鍵カプセルデータ格納部1104に格納された鍵カプセルデータCiの車載機への送信、及び検証鍵格納部1102に格納されて

いる検証鍵Vcの路側機への送信の制御を行う通信制御機能をも有する。

<車載機>車載機1200は、車に搭載され、高速道路の入路ゲート又は出路ゲートに設置された路側機1300等と公開通信路1003を介して無線で通信することにより高速道路の利用料金を自動的に支払うもので、メモリ及びCPU等からなる機器であり、着脱可能なICカードを備える。このICカードは、プリペイドカードの機能を持ち当初所定の金額を示す残額情報が記録されている。また、公開通信路1003は、これを通るデータが悪意ある第三者に盗聴されたり改ざんされたりする危険性が高い通信路である。

【0025】車載機1200は機能的には、個別秘密情報格納部1201と、鍵カプセルデータ保存部1202と、復号データ格納部1203と、比較部1204と、乱数発生部1205と、平文データ格納部1206と、復号部1210と、暗号部1220とを備え、各機能は前記メモリにより、又は前記メモリに格納された制御用プログラムが前記CPUに実行されることにより実現されるものである。

【0026】ここで、個別秘密情報格納部1201は、数百台の車載機毎に異なる車載機個別秘密情報Kiを予め格納しているメモリ領域である。この車載機個別秘密情報Kiは、車載機と路側機との間で残額情報等の通信データをやり取りする際にその通信データを暗号化する鍵として用いられる。鍵カプセルデータ保存部1202は、管理センタ1100から秘密通信路1001を介して入手した鍵カプセルデータCiを格納するメモリ領域である。

【0027】復号部1210は、個別秘密情報格納部1201に格納されている車載機個別秘密情報Kiを用いて路側機1300から送られた暗号化されているデータを所定の秘密鍵暗号アルゴリズムによって復号し、復号により得られるデータの格納のためのメモリ領域である復号データ格納部1203に格納するものである。乱数発生部1205は、チャレンジレスポンス手順により機器認証を行うために乱数データを発生するものである。なお、機器認証のためのチャレンジレスポンス手順については後述する。

【0028】比較部1204は、路側機1300から送られる機器認証のための応答データと乱数発生部1205により発生された乱数データとを比較するものである。平文データ格納部1206は、車載機1200が備えるICカードから読み出した残額情報や車載機のID等、路側機1300に対して送信すべき平文データを格納するメモリ領域である。

【0029】また、暗号部1220は、乱数発生部1205が発生した乱数データ又は平文データ格納部1206に格納されている平文データに対して、個別秘密情報格納部1201に格納されている車載機個別秘密情報K

i を用いて、復号部 1210 と同一の秘密鍵暗号アルゴリズムによって暗号化を施すものである。この他、車載機 1200 は、個別秘密情報格納部 1201 に格納されている車載機個別秘密情報 K i の管理センタ 1100 への送信、管理センタ 1100 からの鍵カプセルデータ C i の受信や、鍵カプセルデータ C i、暗号化した乱数データ又は暗号化した平文データ、チャレンジレスポンス手順により復号データ格納部 1203 に格納されたデータの応答データとしての路側機 1300 への送信や、路側機 1300 からの応答データの受信の制御を行う通信制御機能をも有する。

【0030】<路側機>路側機 1300 は、高速道路の入路ゲート又は出路ゲートに設置される路側機であり、車載機 1200 等と公開通信路 1003 を介して無線で通信することにより高速道路の利用料金を自動的に収受するもので、メモリ及び CPU 等からなる機器である。

【0031】路側機 1300 は機能的には、検証鍵保存部 1301 と、回復型署名検証変換部 1302 と、回復データ格納部 1303 と、平文データ格納部 1304 と、乱数発生部 1305 と、比較部 1306 と、復号データ格納部 1307 と、暗号部 1310 と、復号部 1320 とを備え、各機能は前記メモリにより、又は前記メモリに格納された制御用プログラムが前記 CPU に実行されることにより実現されるものである。

【0032】ここで、検証鍵保存部 1301 は、管理センタ 1100 から秘密通信路 1002 を介して入手した検証鍵 V c を秘密性を保持したまま格納するメモリ領域である。回復型署名検証変換部 1302 は、車載機 1200 から公開通信路 1003 を介して送られる鍵カプセルデータ C i に対して、検証鍵保存部 1301 に格納されている検証鍵 V c を用いて、回復型署名検証変換を行うことにより、車載機個別秘密情報を算出して、メモリ領域である回復データ格納部 1303 に格納するものである。なお、回復型署名検証変換は、管理センタ 1100 においてなされる回復型署名変換に対応するものである。

【0033】平文データ格納部 1304 は、車載機 1200 に対して送信すべき、更新後の残額情報等の平文データを格納するメモリ領域である。乱数発生部 1305 は、チャレンジレスポンス手順により機器認証を行うために乱数データを発生するものである。比較部 1306 は、車載機 1200 から送られる機器認証のための応答データと乱数発生部 1305 により発生された乱数データとを比較するものである。

【0034】暗号部 1310 は、車載機 1200 と同一の秘密鍵暗号アルゴリズムにより、平文データ格納部 1304 に格納されている平文データ、又は乱数発生部 1305 により発生された乱数データに対して、回復データ格納部 1303 に格納されている車載機個別秘密情報を用いて暗号化を施すものである。また、復号部 132

0 は、回復データ格納部 1303 に格納されている車載機個別秘密情報を用いて暗号部 1310 と同一の秘密鍵暗号アルゴリズムにより、車載機 1200 から送られるデータを復号し、メモリ領域である復号データ格納部 1307 に格納するものである。

<回復型署名変換について>上述した回復型署名変換は、例えば楕円曲線上の NR 署名アルゴリズムによりなされる。ここで、楕円曲線上の NR 署名アルゴリズムとは米国電気電子技術者協会 (IEEE) の 1363 作業部会で標準化が進められているデジタル署名方式の一つであり、署名文は、被署名文に対して署名鍵を用いて署名変換したものであり、署名文に対して検証鍵を用いて検証変換を行うと元の被署名文が再現されるという特徴をもつ。

【0035】<楕円曲線上の NR 署名変換>以下、楕円曲線上の NR 署名変換について説明する。楕円曲線とは、(x, y) 平面において、次の数 1 を満足する点 (x, y) の集合である。

$$[数1] \quad y^2 = x^3 + ax + b$$

数 1 において、a、b、x、y は GF(p) の元であり、a、b は定数であり、ここで p は大きな素数である。以下、小文字で示す数は、p 未満の正数を表す。また、大文字は楕円曲線上の点の x、y 座標を表す。

【0036】この楕円曲線上の点であって位数が大きな素因数を含む数となる一つの点をベース点 Q として選ぶ。ここで位数 n とは Q の n 倍の点が G 自身となるような最少の正数である。復号鍵 s は n 以下である正数である。これに対応する暗号鍵 P は Q の s 倍点の座標である。署名対象である被署名文を m とする。

【0037】署名鍵: d

検証鍵: Q 及び P (=sQ)

ここで、署名鍵 d から、検証鍵 P は容易に計算できるが、逆に検証鍵 P と Q から署名鍵 d を計算するのは、前記位数 n が大きいとき非常に困難になるという、いわゆる「楕円曲線上の離散対数問題の困難さ」がこの署名方法の安全性の根拠となっている。楕円曲線の離散対数問題に準拠するこの署名方法によれば、同じ安全性を確保するのに RSA 暗号よりも少ないビット数しか必要としない。なお、これらの署名方法については、「現代暗号」(岡本龍明、山本博資著、産業図書刊、1997 年)に詳しく説明されている。

【0038】ここで、p の具体的な値としては、例えば 160 ビット程度の大きさの数が選ばれる。また、ここで説明した署名鍵 d と、検証鍵 Q 及び P とは、それぞれ上述した管理センタ 1100 の署名鍵格納部 1101 に格納される署名鍵 S c と、検証鍵格納部 1102 に格納される検証鍵 V c とに相当する。

【0039】<署名変換>署名変換は次のように行う。

step 1 乱数 k を発生。

step 2 $W = kQ$ を計算。W の x 座標を W_x とす

る。

step 3 $c1 = Wx \text{ EXOR } m$

ここで、EXORは、ビット毎の排他的論理和を示す演算子とする。

step 4 $c2 = k - d \cdot c1 \pmod{n}$

step 5 $(c1, c2)$ を被署名文 m に対する署名とする。

【0040】＜署名検証変換＞署名検証変換は次のように行う。

step 6 $(c1, c2)$ を受信

step 7 $W = c1P + c2Q$ を計算

step 8 $c1 \text{ EXOR } Wx$ により、被署名文 m が再現される。

【0041】なお、上記ステップ8の結果が m になることは、

$$W = c1P + (k - d \cdot c1)Q$$

$$= c1P + kQ - c1 \cdot (dQ)$$

$$= kQ$$

であることから確認できる。

＜動作＞以下、上述した構成を備える高速道路料金自動收受システム1000の動作について説明する。

【0042】＜概要＞高速道路の入路ゲートにおいては、車載機は路側機に対して車載機IDを無線で送信し、路側機は車載機に対しては、ゲートID、入路時刻等を含む入路情報を無線で送信する。車載機は路側機から入路情報を受信すると、この入路情報をICカードに記録する。

【0043】一方、出路ゲートにおいては、車載機は路側機に対して入路情報と残額情報を無線で送信し、路側機は受信した入路情報に基づいて高速道路の利用料金を計算して、受信した前記残額情報からその利用料金を差引いて残額情報を更新して、更新後の残額情報を車載機に対して無線で送信する。ここでは、管理センタ1100と、1台の車載機1200と、1台の路側機1300との関係に着目して説明する。

【0044】＜検証鍵の配布＞管理センタ1100は、検証鍵格納部1102に格納された検証鍵 Vc を路側機1300に秘密通信路1002を介して送信する。これを受けて路側機1300はその検証鍵 Vc を検証鍵保存部1301に保存する。

＜鍵カプセルデータの作成及び配布＞図2は、管理センタ1100による鍵カプセルデータの作成及び配布動作を示す図である。

【0045】車載機1200は、個別秘密情報格納部1201に予め格納されている車載機個別秘密情報 Ki を秘密通信路1001を介して管理センタ1100に送信する（ステップS2001）。管理センタ1100は、車載機1200から車載機個別秘密情報 Ki を受信し（ステップS2002）、回復型署名変換部1103によりその車載機個別秘密情報 Ki に対して署名鍵格納部

1101に格納されている署名鍵 Sc を用いて上述したNR署名変換を行い、鍵カプセルデータ Ci を作成し鍵カプセルデータ格納部1104に格納する（ステップS2003）。ここで、鍵カプセルデータ Ci は、上述のNR署名変換の説明中の $(c1, c2)$ に相当する。

【0046】鍵カプセルデータ Ci を作成した管理センタ1100は、鍵カプセルデータ格納部1104に格納されている鍵カプセルデータ Ci を秘密通信路1001を介して車載機1200に送信する（ステップS2004）。車載機1200は、管理センタ1100から送信された鍵カプセルデータ Ci を受信して鍵カプセルデータ保存部1202に保存する（ステップS2005）。

【0047】以下、上述した検証鍵の配布と鍵カプセルデータの作成及び配布の完了した状態を初期状態として、ここでは、路側機1300が入路ゲートに設置されているとし、車載機1200が入路ゲートに到達したことから両者間で機器認証及び暗号通信がなされる手順を説明する。なお、初期状態に至るまでの間は、特に高度のセキュリティ管理がなされ、不正な路側機が検証鍵 Vc を入手することは不可能であるものとする。

【0048】＜秘密情報の共有化、機器認証及び暗号通信の手順＞図3は、車載機1200と路側機1300とによる秘密情報の共有化、機器認証及び暗号通信の動作手順を示す図である。

＜秘密情報の共有化＞車載機1200は、鍵カプセルデータ保存部1202に保存している鍵カプセルデータ Ci を、公開通信路1003を介して路側機1300に対して送信する（ステップS3001）。

【0049】これに対して路側機1300は、鍵カプセルデータ Ci を受信し（ステップS3002）、その鍵カプセルデータ Ci に対して、検証鍵保存部1301に格納されている検証鍵 Vc を用いて上述した回復型署名の検証変換を行うことにより、車載機個別秘密情報 Ki' を取り出し回復データ格納部1303に格納する。回復データ格納部1303に格納された車載機個別秘密情報 Ki' は、車載機が正当な鍵カプセルデータを送信した場合には、車載機1200内の個別秘密情報格納部1201に格納されている車載機個別秘密情報 Ki と同じ値となる。即ち、これ以後の機器認証及び暗号通信のために用いられるべき秘密情報が、車載機1200と路側機1300との間で共有化されたことになる。

【0050】＜機器認証＞車載機個別秘密情報を得た後、路側機1300は、乱数発生部1305により乱数 $R1$ を発生し、暗号部1310によりこの乱数 $R1$ に対して回復データ格納部1303に格納されている車載機個別秘密情報 Ki' を鍵として用いて暗号化し、この暗号化の結果として生じたデータ（以下「暗号化乱数 $E1$ 」という。）を、公開通信路1003を介して車載機1200に送信する（ステップS3004）。

【0051】これに対応して車載機1200は、暗号化

乱数E1を受信し、復号部1210により暗号化乱数E1を入力暗号文としてこれに対して個別秘密情報格納部1201に格納されている車載機個別秘密情報Kiを復号鍵として用いて復号し、この復号の結果として生じたデータ（以下「応答データD1」という。）を復号データ格納部1203に格納し、この応答データD1を公開通信路1003を介して路側機1300に送信する（ステップS3005）。

【0052】これに対応して応答データD1を受信した路側機1300は、比較部1306により、応答データD1と、ステップS3004において乱数発生部1305に生成された乱数R1とを比較する（ステップS3006）。この比較により両者が一致するならば、路側機1300は車載機1200が正当な機器であると判断できる。即ち、一致すれば、以後の機器認証及び暗号通信の処理は続行されるが、一致しなければ、車載機1200が不正なものとみなされるため、図3に示す処理は中止され、例えば、車載機1200を搭載する車の撮影等、不正に対する対抗措置がなされる。

【0053】なお、車載機1200の正当性が確認できたことから、回復データ格納部1303に格納されている車載機個別秘密情報Ki'と車載機1200内の個別秘密情報格納部1201に格納されている車載機秘密情報Kiと同値であること、及び、暗号部1310の暗号化アルゴリズムと復号部1210の復号アルゴリズムとが呼応するものであることが推定できる。

【0054】このように、ステップS3004～S3006により路側機1300は車載機1200の正当性を認証するのであるが、これに続いて、逆に車載機1200から路側機1300の正当性を以下に示す手順で認証する（ステップS3007～ステップS3009）。車載機1200は、乱数発生部1205により乱数R2を発生し、暗号部1220によりこの乱数R2に対して個別秘密情報格納部1201に格納されている車載機個別秘密情報Kiを暗号鍵として用いて暗号化し、この暗号化の結果として生じたデータ（以下「暗号化乱数E2」という。）を、公開通信路1003を介して路側機1300に送信する（ステップS3007）。

【0055】これに対応して路側機1300は、暗号化乱数E2を受信し、復号部1320により暗号化乱数E2を入力暗号文としてこれに対して回復データ格納部1303に格納されている車載機個別秘密情報Ki'を復号鍵として用いて復号し、この復号の結果として生じたデータ（以下「応答データD2」という。）を復号データ格納部1307に格納し、この応答データD2を公開通信路1003を介して車載機1200に送信する（ステップS3008）。

【0056】これに対応して応答データD2を受信した車載機1200は、比較部1204により、応答データD2と、ステップS3007において乱数発生部120

5に生成された乱数R2とを比較する（ステップS3009）。この比較により両者が一致するならば、車載機1200は路側機1300が正当な機器であると判断できる。即ち、一致すれば、以後の暗号通信の処理は続行されるが、一致しなければ、路側機1300が不正なものとみなされるため、図3に示す処理は中止される。

【0057】ここで説明した手順、即ち、機器認証のために暗号化乱数E1と応答データD1とを送信し合う手順、及び機器認証のために暗号化乱数E2と応答データD2とを送信し合う手順が、いわゆるチャレンジレスポンス手順である。

<暗号通信>機器認証が成功した後は、車載機1200は、車載機IDを平文データ格納部1206に格納し、暗号部1220により、平文データ格納部1206に格納されているその車載機IDを平文として、これに対して個別秘密情報格納部1201に格納されている車載機個別秘密情報Kiを暗号鍵として用いて暗号化し、その結果として生じた暗号文m1を公開通信路1003を介して路側機1300に送信する（ステップS3010）。

【0058】これに対応して路側機1300は、暗号文m1を受信し、復号部1320によりこの暗号文m1に対して回復データ格納部1303に格納されている車載機個別秘密情報Ki'を復号鍵として用いて復号し、復号結果を復号データ格納部1307に格納する（ステップS3011）。これにより、路側機1300は、車載機1200の車載機IDを得ることができる。

【0059】また、路側機1300は、入路情報を平文データ格納部1304に格納し、暗号部1310により、平文データ格納部1304に格納されているその入路情報を平文として、これに対して回復データ格納部1303に格納されている車載機個別秘密情報Ki'を暗号鍵として用いて暗号化し、その結果として生じた暗号文m2を公開通信路1003を介して車載機1200に送信する（ステップS3012）。

【0060】これに対応して車載機1200は、暗号文m2を受信し、復号部1210によりこの暗号文m2に対応して個別秘密情報格納部1201に格納されている車載機個別情報Kiを復号鍵として用いて復号し、復号結果を復号データ格納部1203に格納する（ステップS3013）。これにより、車載機1200は、入路情報を得ることができる。

【0061】なお、ここでは、入路ゲートにおける車載機1200と路側機1300と間でのデータの送受信について説明したが、出路ゲートにおいても図3に示す手順と同様の手順により、車載機1200とある路側機との間でデータが送受信される。

<考察>上述した高速道路料金自動收受システム1000によれば、次のような効果が得られる。

【0062】第1に、路側機は、各車載機についての個

別の秘密情報である車載機個別秘密情報を、車載機から送信される鍵カプセルデータから復元することができるので、全ての車載機について、車載機IDと車載機個別秘密情報とを対応づけて予め記憶しておく必要がなく、これにより路側機が不正に侵入された場合に対する安全性が高まっている。

【0063】第2に、路側機側が車載機個別秘密情報を復元するためには、正当な路側機しか知らない秘密データ、即ち検証鍵 V_c を必要とするので、このことから車載機は、路側機が正当な機器か否かを認証することができ、この結果として、不正な路側機を用いた不正行為が防止できる。第3に、鍵カプセルデータを作成するのに回復型署名変換を用いるので、路側機が不正に侵入され解析されて、管理センタの検証鍵 V_c が知得されたとしても、検証鍵 V_c からは、管理センタの署名鍵 S_c が導き出せないため、鍵カプセルデータの偽造は行えない。

【0064】第4に、楕円曲線上の離散対数問題に準拠する回復型署名方法を用いるので、RSA暗号を用いる場合と比較して、安全性を保ったままでデータ量を削減できる。

<補足>以上、本発明に係る機器認証及び暗号通信システムについて、実施形態である高速道路料金自動收受システム1000を例に挙げて説明したが、本発明はこのような実施形態に限られないことは勿論である。即ち、

(1) 本発明に係る機器認証及び暗号通信システムは、例えば携帯電話システム等、複数のユーザ側機器と、1又は複数のシステム側機器との間で機器認証と暗号通信とを要するシステムにおいて広く適用できるものである。本実施の形態に示した高速道路料金自動收受システム1000における車載機はユーザ側機器に相当し、路側機はシステム側機器に相当する。

【0065】例えば、このユーザ側機器は、数十メガバイトの記憶容量をもち機器認証及び暗号通信のための制御回路を内蔵する半導体メモリであるメモリカードであり、システム側機器は、そのメモリカードから暗号化を施されて送られるデータを読み出し復号して利用するパーソナルコンピュータ等の機器であることとすることができる。これによれば、メモリカードが個別秘密情報を保有し、これを暗号鍵として用いて暗号化してデータを出力することとなるが、この場合の暗号化は、公開鍵暗号アルゴリズムと比較してアルゴリズムの単純な秘密鍵暗号アルゴリズムにより行われるため、小型で計算能力が低いメモリカードによっても、実使用に耐える速度でのデータの暗号化等が可能となる。また、各メモリカードについて、メモリカード毎に異なる個別秘密情報に対する鍵カプセルデータを、管理システムが予め各メモリカード内に記録しておけば、たとえパーソナルコンピュータ等の機器が不正に侵入され解析されたとしても、メモリカード内の鍵カプセルデータを偽造することが不可能となる。

(2) 本実施の形態において示した高速道路料金自動收受システム1000では、車載機と路側機とは無線で通信されることとしたが、本発明は、ユーザ側機器とシステム側機器とのデータ通信が無線でなされることに限定されない。

【0066】また、本実施の形態において、管理センタと、ユーザ側機器又はシステム側機器との間でのデータ通信は安全な秘密通信路により行われることとしたが、この秘密通信路は、必ずしも電氣的な通信路である必要はない。例えば物理的に安全な装置を介することにより、データのやり取りがなされることとしてもよい。また、本実施の形態において、車載機毎に異なる車載機個別秘密情報を予め格納していることとしたが、本発明に係る機器認証及び暗号通信システムにおいては、予め管理センタにより、ユーザ側機器毎に異なるように個別秘密情報が作成されて、その個別秘密情報に対応する鍵カプセルデータと共に各ユーザ側機器に配布されていることとしてもよい。

(3) 本実施の形態においては、鍵カプセルデータを作成するのに回復型署名を用いること、即ち、管理センタは秘密鍵である署名鍵を用いて個別秘密情報に対して回復型署名を行うことにより鍵カプセルデータを作成し、システム側機器は、公開鍵である検証鍵を用いて鍵カプセルデータから個別秘密情報を復元することとしたが、前回回復型署名の代わりに公開鍵暗号を用いることとしても、システム側機器が、個々のユーザ側機器の個別秘密情報をそのユーザ側機器の識別番号等と対応づけて記憶しておく必要がないという上記考察に示した第1の効果は得られる。公開鍵暗号を用いる場合は、管理センタは、ユーザ側機器の個別秘密情報に対して公開鍵を用いて公開鍵暗号変換を行い鍵カプセルデータを作成してユーザ側機器に配布し、また、その公開鍵に対応する秘密鍵をシステム側機器に配布しておき、システム側機器は、管理センタから配布された秘密鍵を用いて、ユーザ側機器から送信される鍵カプセルデータから公開鍵復号変換により個別秘密情報を取り出すことになる。

【0067】また、本実施の形態においては、楕円曲線上の離散対数問題に基づく回復型署名を用いることとしたが、これを他の回復型署名に代えても、上記考察に示した第3の効果は得られる。

(4) 本実施の形態においては、車載機と路側機とが相互に機器認証を行うこととしたが、一方の機器についての機器認証のみを行い、他方についての機器認証は行わないこととしてもよい。

【0068】また、本実施の形態においては、車載機から路側機に対して暗号文 m_1 が送られ、逆に路側機から車載機に対して暗号文 m_2 が送られることとしたが、送信順序はこれに限定されず、また、暗号文の送信が必ずしも双方向に行われなければならないことはない。また、本発明は、本実施の形態において説明したチャレン

ジレスポンス手順の一例に限定されることはなく、ユーザ側機器とシステム側機器との間で、共有した個別秘密情報を鍵として用いて暗号化又は復号を行うことによって機器認証を行うものであればよい。例えば、ユーザ側機器とシステム側機器のうち一方を機器A、他方を機器Bとすると、機器Aが乱数を機器Bに送信し、機器Bは受け取った乱数に対して個別秘密情報を鍵として用いて暗号化を行い、暗号化により生成されるデータを機器Aに返信し、機器Aは先に送信した乱数に対して個別秘密情報を鍵として用いて暗号化を行い、この暗号化の結果として生成されるデータと、機器Bから送られたデータとが一致するかどうかを判断することにより機器認証を行うこととしてもよい。

(5) 本実施の形態に示した高速道路料金自動収受システム1000の管理センタ、車載機又は路側機による動作手順(図2、図3に示した手順等)を、汎用のコンピュータ又はプログラム実行機能を有する家電機器に実行させるためのコンピュータプログラムを、記録媒体に記録し又は各種通信路等を介して、流通させ頒布することもできる。かかる記録媒体には、ICカード、光ディスク、フレキシブルディスク、ROM等がある。流通、頒布されたコンピュータプログラムは、プログラム実行機能を有する家電機器やパーソナルコンピュータ等にインストール等されることにより利用に供され、家電機器やパーソナルコンピュータは、当該コンピュータプログラムを実行して、本実施の形態に示したような機器認証及び暗号通信に関する諸機能を実現する。

【0069】

【発明の効果】以上の説明から明らかなように本発明に係る機器認証及び暗号通信システムは、機器認証及び暗号通信を行う機器認証及び暗号通信システムであって、各ユーザ側機器毎に異なる個別秘密情報それぞれに対して、所定の変換を行うことにより鍵カプセルデータを作成して、各鍵カプセルデータを該当ユーザ側機器に配布し、前記各鍵カプセルデータから前記各個別秘密情報を復元するために用いる1つの所定鍵をシステム側機器に配布する管理装置と、各ユーザ側機器は、前記個別秘密情報を記憶しており、機器認証及び暗号通信を行うに際して、前記管理装置により配布された前記鍵カプセルデータをシステム側機器に送信する複数のユーザ側機器と、前記ユーザ側機器から前記鍵カプセルデータを受信すると、前記管理装置により配布された前記所定鍵を用いて当該鍵カプセルデータから前記個別秘密情報を復元するシステム側機器とを備え、前記ユーザ側機器は前記記憶している個別秘密情報を鍵として用い、前記システム側機器は前記復元した個別秘密情報を鍵として用いて、秘密鍵暗号アルゴリズムに基づく暗号化又は復号を行うことにより、前記機器認証及び暗号通信を行うことを特徴とする。

【0070】これにより、システム側機器は、ユーザ側

機器から送られる鍵カプセルデータからユーザ側機器毎に異なるものである個別秘密情報を復元するので、全てのユーザ側機器について、個別秘密情報とユーザ側機器のID等と対応づけて記憶していなくても、ユーザ側機器との間で機器の正当性の認証と暗号通信とを行うことができる。従って、システム側機器には全てのユーザ側機器についての個別秘密情報を記憶しないようにすることができるため、この場合、悪意ある者がシステム側機器に不正に侵入し解析を行ったとしても、その者は全てのユーザ側機器についての個別秘密情報を入手することはできない。

【0071】ここで、前記管理装置は、回復型署名変換方法における署名鍵とこれに対応する検証鍵とを予め記憶しており、前記所定の変換は、前記署名鍵を用いてなされる回復型署名変換であり、前記所定鍵は、前記検証鍵であり、前記システム側機器は、前記所定鍵を用いて前記回復型署名変換に対応する回復型署名検証変換を行うことにより当該鍵カプセルデータから前記個別秘密情報を復元することとすることもできる。

【0072】これにより、鍵カプセルデータは回復型署名変換により作成されるため、システム側機器への不正な侵入及び解析により、その回復型署名についての署名検証変換用の検証鍵を得ることはできたととしても、その検証鍵からは回復型署名変換に用いる署名鍵が導き出せないで、悪意ある者による鍵カプセルデータの偽造が不可能となる。

【0073】また、前記機器認証は、前記ユーザ側機器及び前記システム側機器のうち的一方である第1機器が乱数データを前記秘密鍵暗号アルゴリズムに基づき暗号化して、他方の第2機器に送信し、これを受信した第2機器が暗号化された乱数データを前記秘密鍵暗号アルゴリズムに基づき復号して応答データを作成し第1機器に返信し、前記応答データを受信した第1機器が当該応答データと前記乱数データとを比較することにより行われることとすることもできる。

【0074】これにより、システム側機器が鍵カプセルデータから復元した個別秘密情報をユーザ側機器と共有することによって、その個別秘密情報を共通の秘密鍵として秘密鍵暗号アルゴリズムに基づいてチャレンジレスポンス手順によりユーザ側機器又はシステム側機器の正当性の認証を行うので、認証が成功すれば、個別秘密情報が正しく共有されていることが確認できる。また、上記したように悪意ある者による鍵カプセルデータの偽造が不可能であることを前提とすれば、このチャレンジレスポンス手順によりユーザ側機器の正当性の認証を行う場合における認証の確かさは高いものとなる。

【0075】また、前記回復型署名変換及び前記回復型署名検証変換は、楕円曲線理論に基づくものであることとすることもできる。これにより、システムの安全性を低下させることはなく、個別秘密情報を共有化するため

にユーザ側機器からシステム側機器に送信される鍵カプセルデータのデータ量を縮小化することができる。

【0076】また、前記ユーザ側機器は、車に備えられる車載機であり、前記システム側機器は、道路に設けられた路側機であり、前記ユーザ側機器と前記システム側機器との間でのデータ送受信は、前記ユーザ側機器が前記システム側機器の付近を通過する際に行われることとすることもできる。これにより、車載機が搭載された複数の車について、そのいずれかが道路に設置された路側機の付近を通過する際に、車載機と路側機との間で、セキュリティを確保しつつ秘密鍵を共有することが可能となる。従って、車載機と路側機との間で、秘密鍵暗号アルゴリズムによる暗号化又は復号を用いる機器認証や暗号通信を行うことができるため、公開鍵暗号アルゴリズムを用いる場合よりも比較的高速に機器認証及び暗号通信が行え、この結果、路側機が設置された箇所の付近における車の渋滞を防止することができる。

【0077】また、前記ユーザ側機器と前記システム側機器との間での機器認証は、相互に相手側機器を認証するものであり、前記ユーザ側機器と前記システム側機器との間での暗号通信は、双方向に行われることとすることもできる。これにより、ユーザ側機器は鍵カプセルデータを管理センタから受け取った正当な機器であり、システム側機器は検証鍵を管理センタから受け取った正当な機器であることが相互に認証でき、また、公開された通信路を介して安全にデータ通信を送受信することができる。

【0078】また、前記管理装置は、複数の前記個別秘密情報を該当ユーザ側機器に配布し、前記ユーザ側機器が記憶している前記個別秘密情報は、前記管理装置から配布されたものであることとすることもできる。これにより、管理センタは、個別秘密情報をユーザ側機器に配布する前に、その個別秘密情報に対して回復型署名変換を行うことにより鍵カプセルデータが作成できるため、ユーザ側機器から個別秘密情報を受信するための手段を備える必要がなく、簡易な構成で実現できる。

【0079】また、前記管理装置は、公開鍵暗号方法における公開鍵とこれに対応する秘密鍵とを予め記憶しており、前記所定の変換は、前記公開鍵を用いてなされる公開鍵暗号変換であり、前記所定鍵は、前記秘密鍵であり、前記システム側機器は、前記所定鍵を用いて前記公開鍵暗号変換に対応する復号変換を行うことにより当該鍵カプセルデータから前記個別秘密情報を復元することとすることもできる。

【0080】これにより、システム側機器は、管理センタから配布された秘密鍵を用いて個別秘密情報を復元することができるため、全てのユーザ側機器についての個別秘密情報を予め記憶しておく必要がない。全ての個別秘密情報を予め記憶しなければ、システム側機器が不正に侵入され解析された場合においても、全てのユーザ側

機器の個別秘密情報が暴露されることがないのでシステムの安全性が高まる。

【0081】また、本発明に係る鍵配送方法は、機器認証及び暗号通信用の鍵である個別秘密情報を記憶する複数のユーザ側機器のいずれかから、システム側機器に対して前記個別秘密情報を配送する鍵配送方法であって、各ユーザ側機器についての前記個別秘密情報に対して回復型署名変換を行うことにより鍵カプセルデータを作成して、該当ユーザ側機器に配布する鍵カプセルデータ作成及び配布ステップと、前記回復型署名変換に対応する署名検証変換に用いる検証鍵を前記システム側機器に配布する検証鍵配布ステップと、前記ユーザ側機器によりなされ、前記鍵カプセルデータ作成及び配布ステップにより配布された前記鍵カプセルデータを前記システム側機器に送信する鍵カプセルデータ送信ステップと、前記鍵カプセルデータ送信ステップにより送信された鍵カプセルデータを受信し、前記検証鍵配布ステップにより配布された前記検証鍵を用いて当該鍵カプセルデータから前記個別秘密情報を復元する鍵復元ステップとを含むことを特徴とする。

【0082】これにより、システム側機器が全てのユーザ側機器について、個別秘密情報とユーザ側機器のID等と対応づけて記憶していなくても、ユーザ側機器との間で機器の正当性の認証と暗号通信とを行うことができ、また、システム側機器への不正な侵入及び解析により不正に回復型署名についての署名検証変換用の検証鍵を得ることはできたととしても、その検証鍵からは回復型署名変換に用いる署名鍵が導き出せないで、悪意ある者による鍵カプセルデータの偽造が不可能となる。

【図面の簡単な説明】

【図1】本発明の実施の形態に係る高速道路料金自動收受システム1000の主要部分の機能構成図である。

【図2】高速道路料金自動收受システム1000における管理センタ1100による鍵カプセルデータの作成及び配布動作を示す図である。

【図3】高速道路料金自動收受システム1000における車載機1200と路側機1300とによる秘密情報の共有化、機器認証及び暗号通信の動作手順を示す図である。

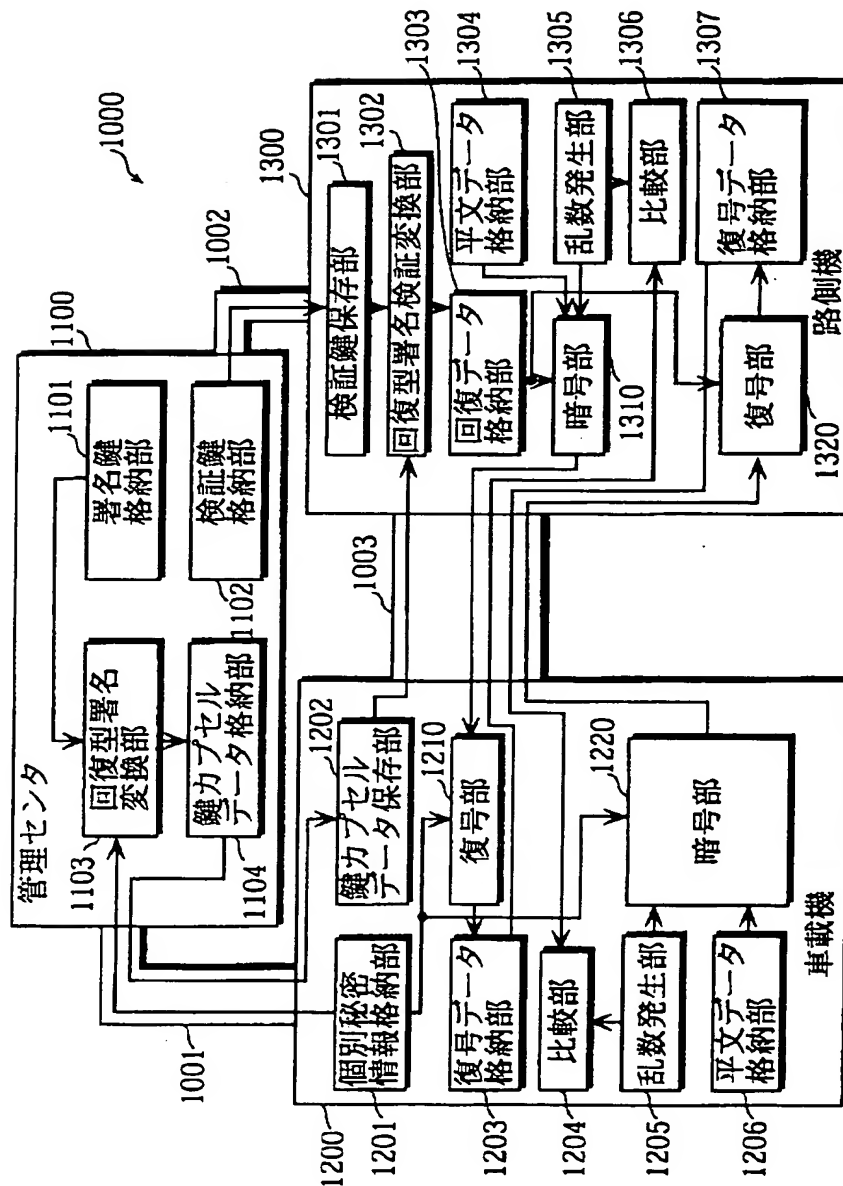
【符号の説明】

1000	高速道路料金自動收受システム
1001、1002	秘密通信路
1003	公開通信路
1100	管理センタ
1101	署名鍵格納部
1102	検証鍵格納部
1103	回復型署名変換部
1104	鍵カプセルデータ格納部
1200	車載機
1201	個別秘密情報格納部

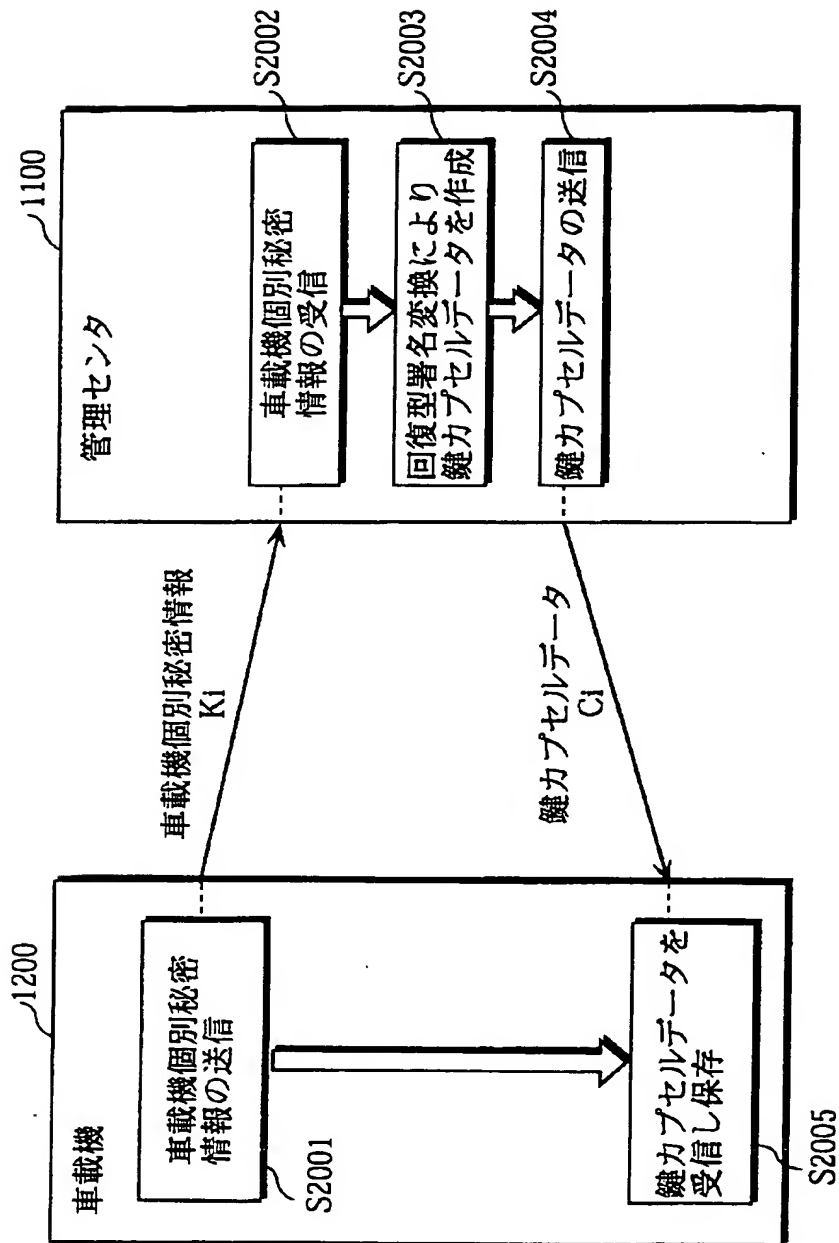
1202 鍵カプセルデータ保存部
 1203 復号データ格納部
 1204 比較部
 1205 乱数発生部
 1206 平文データ格納部
 1210 復号部
 1220 暗号部
 1300 路側機
 1301 検証鍵保存部

1302 回復型署名検証変換部
 1303 回復データ格納部
 1304 平文データ格納部
 1305 乱数発生部
 1306 比較部
 1307 復号データ格納部
 1310 暗号部
 1320 復号部

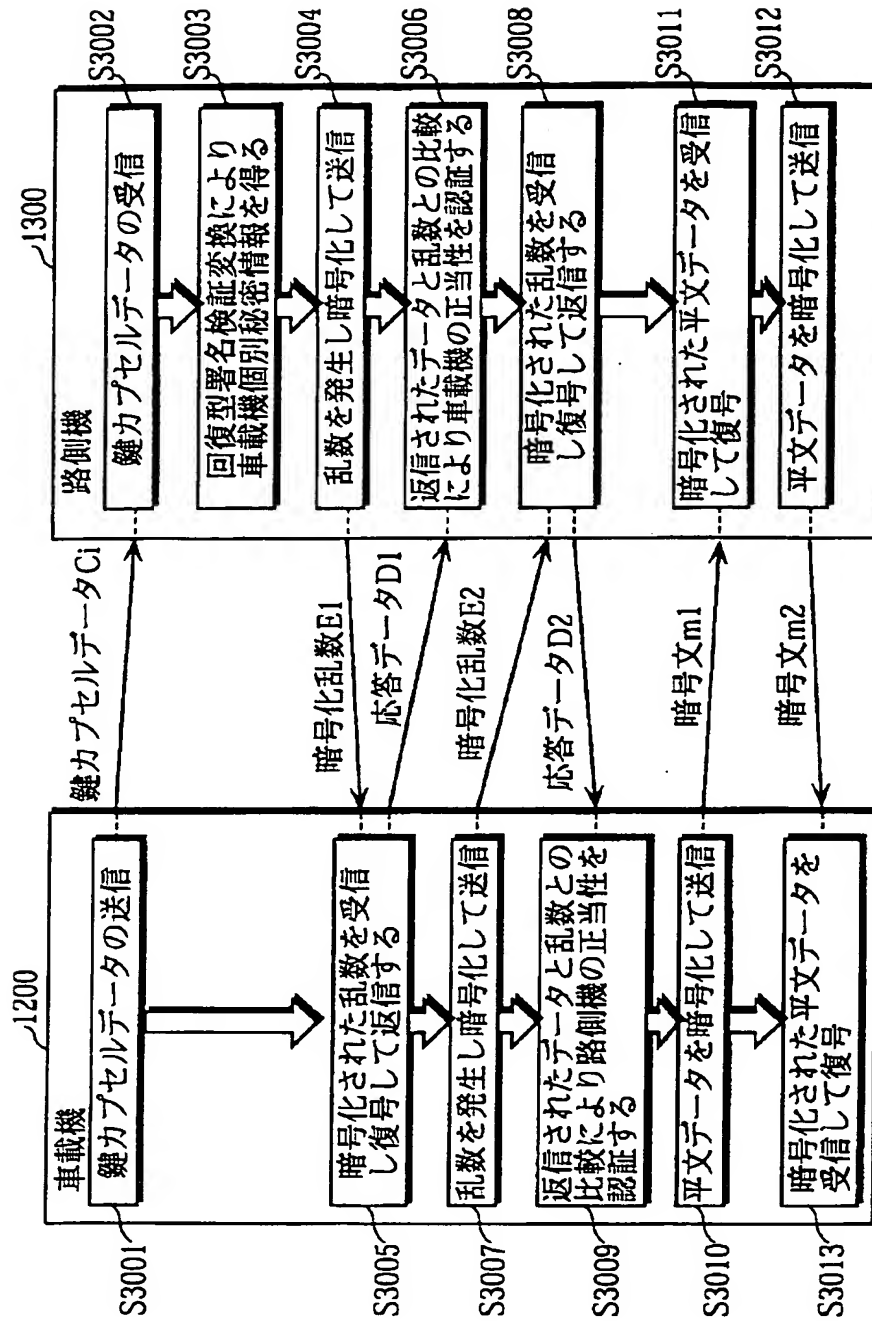
【図1】



【図 2】



【図 3】



フロントページの続き

(51) Int. Cl. 6

識別記号

F I

H 0 4 L 9/00

6 7 5 D